The psychology of internet fraud victimisation

Norris, Gareth; Brookes, Alexandra; Dowell, David

Published in:
Journal of Police and Criminal Psychology

DOI:
10.1007/s11896-019-09334-5

Publication date:
2019

Citation for published version (APA):
Norris, G., Brookes, A., & Dowell, D. (2019). The psychology of internet fraud victimisation: A systematic review. *Journal of Police and Criminal Psychology*, *34*(3), 231-245. https://doi.org/10.1007/s11896-019-09334-5

Journal of Police and Criminal Psychology
https://doi.org/10.1007/s11896-019-09334-5

The Psychology of Internet Fraud Victimisation: a Systematic Review

Gareth Norris[1] · Alexandra Brookes[1] · David Dowell[2]

Abstract
Existing theories of fraud provide some insight into how criminals target and exploit people in the online environment; whilst reference to psychological explanations is common, the actual use of established behavioural theories and/or methods in these studies is often limited. In particular, there is less understanding of why certain people/demographics are likely to respond to fraudulent communications. This systematic review will provide a timely synthesis of the leading psychologically based literature to establish the key theories and empirical research that promise to impact on anti-fraud policies and campaigns. Relevant databases and websites were searched using terms related to psychology and fraud victimisation. A total of 44 papers were extracted and 34 included in the final analysis. The studies range in their scope and methods; overall, three main factors were identified: message ($n = 6$), experiential ($n = 7$), and dispositional ($n = 21$), although there was some overlap between these (for example, mapping message factors onto the dispositional traits of the victim). Despite a growing body of research, the total number of studies able to identify specific psychological processes associated with increased susceptibility to online fraud victimisation was limited. Messages are targeted to appeal to specific psychological vulnerabilities, the most successful linking message with human factors, for example, time-limited communications designed to enact peripheral rather than central information processing. Suggestions for future research and practical interventions are discussed.

Keywords Fraud · Internet fraud · Scam · Compliance · Psychology

Introduction

The FBI's Internet Crime Complaint Center (IC3) recently reported figures that show Internet-enabled theft, fraud, and exploitation being responsible for $2.7 billion in financial losses in 2018 (FBI 2018). The annual Internet Crime Report shows that IC3 received 351,936 complaints last year—nearly 1000 per day—with non-payment/non-delivery scams, extortion, and personal data breaches the most frequently reported. The most financially costly were business email compromise, romance or confidence fraud, and investment scams. Internet-based fraud was the fastest growing crime in the UK in 2015–2016, with 3.25 million victims each year and an annual combined loss of £3.6 billion (Button et al. 2016). Estimates indicate 4.7 million incidents of fraud and computer misuse were experienced by adults aged 16 and over in England and Wales for the survey year ending September 2017 (ONS, 2017). Button and Cross (2017; p. 23) provide a summary on the rising role of technology in perpetuating these crimes: '[i]ndeed it is estimated globally there are 29 billion spam emails daily and that the email virus rate is 1 in 196 and phishing emails are 1 in 392'. The on-going infiltration and reliance on technology into our daily lives is likely to see this trend increase in the short-to-medium term until we develop suitable strategies to stay secure online.

However, despite current efforts to educate individuals on the way in which criminals operate online, millions of these fraudulent activities—from phishing attempts to 'lonely hearts' scams—are responded to each year (NAO 2017); inherent human weaknesses for incentive-driven behaviours seemingly make many of these scams too alluring to resist. For example, priming individuals with images of money has been shown to reduce helpfulness towards others and increase isolation in tasks involving new acquaintances (Vohs et al. 2006). Similarly, financial decisions elicit different brain structures to similar non-financial rewards (Knutson et al. 2000). Anecdotally, we know that fraud-related messages are designed to exploit certain behavioural and demographic 'weaknesses', for example, impulsiveness and/or loneliness

✉ Gareth Norris
ggn@aber.ac.uk

[1] Aberystwyth University, Aberystwyth, UK

[2] St. Andrews University, St. Andrews, UK

Published online: 02 July 2019

(Duffield and Grabosky 2001). Button et al. (2009) note that when considering the perpetrators of fraud, '[…] there is only limited data available. Even the law enforcement community does not always know the background of the perpetrators.' (p. 13). Significantly, the existing fraud literature is limited in scope in terms of exploring the 'how' and the 'why'—in precisely what way they influence individual decision-making processes? Thus, this systematic review aims to connect some of these methodological and conceptual links to establish how message, experiential, and dispositional factors may influence an individual's cognitive processing associated with increased likelihood for Internet fraud victimisation.

Previous Reviews

There are a number of reviews in the wider online/consumer fraud area, although the focus for many is age as a risk factor. Jackson's (2017) evaluation is predominantly aimed at methodological and prevalence issues and suggests a lack of knowledge of risk factors in the financial exploitation of older people increases propensity for fraud. More recently, a review by Burnes et al. (2017) expands upon many of these points to also include susceptibility to web scams. Incorporating the wider issue of consumer fraud, Ross et al. (2014) attempt to dispel some of the myths regarding age-related victimisation and increased vulnerability. They document six key areas where older people are more likely to be disproportionately exploited by fraudsters, for example, slower cognitive processing and increased trust. However, Ross et al. suggest that age can also act as a protective factor in the sense that older people are less likely to use the Internet for financial transactions. In particular, they caution that vulnerability does not equal prevalence; Ross et al. conclude that psychological research in this area must not overly stereotype older people in the sense that policies designed to reduce victimisation mistakenly create further opportunities for crime.

A recently published report evaluation of fraud typologies and victims by the UK National Fraud Authority (NFA) highlights how victims are selected, approach strategies, and profiles of victims (Button et al. 2016). This report identifies a number of research articles which indicate that targeting individual susceptibility to fraud is a key feature of many scams; for example, using time-limited responses to limit the amount of deliberation. Risk taking and low self-control are also identified as additional personality factors linked to characteristics of fraud victims. The report also goes some way to dispel the myth that older people are more probable victims (although they are more likely to experience fraud than theft or robbery). Lower levels of reporting may be more apparent in older victims—whether they knew the fraud had taken place or not—with those who blamed themselves also being less likely to report. Significantly, active social networks encouraged reporting; these may be less extensive in some older populations. Ultimately, Button et al. caution that: '[…] what is striking about of [sic] the scams is that the profiles cover almost everybody; hence almost anyone could become the victim of a scam' (p. 24). Consequently, although we can observe some small variations in demographics of fraud victims (e.g. age, gender, SES), it appears that individual psychological differences are likely to be the key factor in explaining why some people are more likely to arrive at erroneous decisions in responding to fraudulent online messages.

Theoretical and Conceptual Issues

The majority of previous research conducted in this area predominantly focus on the persuasive influence of the scam message employed by the fraudster (see Chang and Chong 2010) or the knowledge of scams held by the potential victim (see Harrison et al. 2016a). The purpose of this systematic review is to extend that focus to incorporate variables related to individual psychological differences, i.e. those which make people more vulnerable to be deceived by fraudulent communications (see Judges et al. 2017). Research by Modic and colleagues has highlighted individual differences to scam compliance through the lens of susceptibility to persuasion and wider theoretical links with social influence (see Modic et al. 2018; Modic and Lea 2013). The development of the Susceptibility to Persuasion (StP) scale has demonstrated good construct validity in relation to self-report scam plausibility across large samples. The second iteration (StP-II; see Modic et al. 2018) incorporates 10 subscales measuring individual differences in a range of mechanisms, including sensation seeking, risk preferences, and social influence. However, we are still some way from achieving a robust and testable model of online fraud susceptibility.

Dispositional factors currently assessed in the literature predominantly focus on demographic factors, such as age, gender, income, and education (Purkait et al. 2014), in conjunction with individual characteristics, such as low self-control (Holtfreter et al. 2008), high levels of perceived loneliness (Buchanan and Whitty 2014), and impulsivity (Pattinson et al. 2011). The application of Petty and Cacioppo's (1986) elaboration likelihood model (ELM) to explain how psychological mechanisms impact deception likelihood is common (see Vishwanath et al. 2011), although few have applied this theoretical model to explore how dispositional factors influence an individual's cognitive processing associated with victimisation. Similarly, there are a limited number of experimental designs or use of large secondary data sets in this field, both of which would provide the vital understanding of 'how' these influences occur. Upon reflection, much of the literature exploring dispositional factors and

vulnerability to fraud is limited in scope in terms of understanding the psychological mechanisms that lead people to become victims of these scams. Without sufficient grounding in established psychological mechanisms, attempts to prevent or limit victimisation will likely underperform. The aim of this systematic review is to collate and analyse the key research in relation to the psychology of Internet fraud to ascertain the baseline theoretical and research knowledge in this growing area, focusing on established psychological theories and empirically based methodologies.

Methodology

Objectives To examine the extent to which psychological theories have been empirically tested to explain Internet fraud victimisation through a systematic review of the literature. The primary focus is upon understanding the literature which relates to how victims respond to fraudulent communications as opposed to the offender. However, as Button, Lewis, and Tapley (2009, p. 15) note: '[t]he growing literature upon different types of fraud provides much information on the techniques of fraudsters. These diverse range of tactics used [can] be considered under three sub-headings, victim selection techniques, perpetration strategies and finally detection avoiding strategies':

- Victim selection techniques concern the strategies that fraudsters use to contact their victims, e.g. email or virus.
- Perpetration strategies: once the victim has been identified, these are the techniques used by fraudsters to secure money or identity, e.g. legitimate appearance of an email.
- Detection avoidance techniques: techniques used by fraudsters that would minimise their risk of getting caught/sentenced, e.g. making reporting unlikely if ask for a small sum of money.

It is the first two of these that is the focus of this review and primarily the aim is to consolidate our understanding of the psychological mechanisms by which perpetrator (message) and victim (respondent) interact.

Search Methods Multiple investigators (GN and AB) independently screened both titles and abstracts and relevant full-text articles from the following databases: PsychINFO, ProQuest, International Bibliography of the Social Sciences; Applied Social Science Index and Abstracts, Sociological Abstracts; Sage Criminology; Criminal Justice Abstracts, alongside grey literature from Dissertation Abstracts Online and COS Conference Paper Index. Figure 1 shows the flow diagram outlining the search and exclusion process conforming to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines (Moher et al. 2009). Full technical data for the systematic review is included in *Appendix A*.

Inclusion Criteria The key inclusion criteria were that the paper should be an empirical examination of an established psychological theory relating to online fraud. In order to minimise more general commentary and published statistics articles, we restricted our search criteria to peer-reviewed journal articles, conference presentations, and book chapters in English. Both quantitative and qualitative studies were acceptable, but the latter should employ a recognised analysis technique, for example, interpretive phenomenological analysis (IPA), as opposed to more anecdotal commentaries of cases, scams, etc.

Exclusion Criteria There were a large number of articles extracted and screened full text before being rejected as not fulfilling the inclusion criteria ($n = 1036$). The majority of these articles purported to include psychological theories and/or measures (for example, personality). Additional exclusions included other fraud types (e.g. corporate or academic fraud), those not focusing on the individual or individual factors (e.g. socialisation), and did not include at least one established and testable psychological theory (e.g. loneliness).

Data Collection and Analysis

Main Results A total of 1299 initial papers were extracted; 39 papers were included in the final search after the exclusion criteria were applied and an additional 5 equivocal items also added ($n = 44$) (see Fig. 1). From this, a further 10 were excluded by a third author (DD) due to not including an established psychological theory and/or were theoretical models or existing reviews (i.e. not empirical studies). The final number of reviewed articles was 34. The studies range in their scope and methods; overall, three main factors were identified: message, experiential, and dispositional (see Fig. 2).

Meta-analysis Given the diverse nature of the theoretical background and unrelated outcome measures from each study, a meta-analysis of the findings is not appropriate.

Summary of Studies

Modic and Lea (2013) regard Internet fraud as a staged process, involving: '[…] plausibility, interaction with a fraudster, and losing utility to fraud' (p. 15); once an offer is deemed plausible, the later stages are therefore more likely to be forthcoming. The review highlighted some broad groupings under which the empirical research in this area has been targeted. The key variables associated with decisions as to whether or not to decide whether information via the internet is plausible

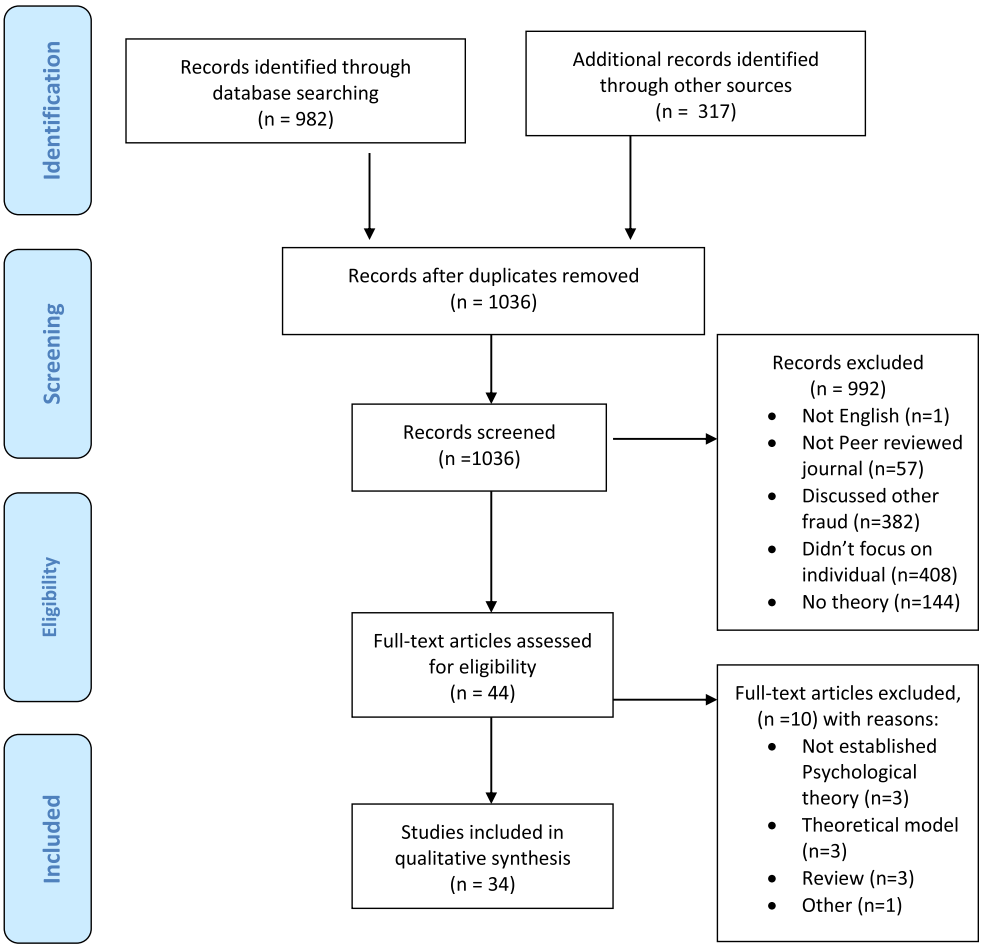

Fig. 1 PRISMA flow diagram for identifying psychologically based studies into Internet-based fraud

can be divided into two key areas: *deceiver* and *receiver* influence (see Fig. 1). These categories represent both the *content* of the message and the way in which it *interacts* with the target. The receiver characteristics can also be further divided into two distinct elements: *experiential* and *dispositional* factors. Experiential factors relate to the person's

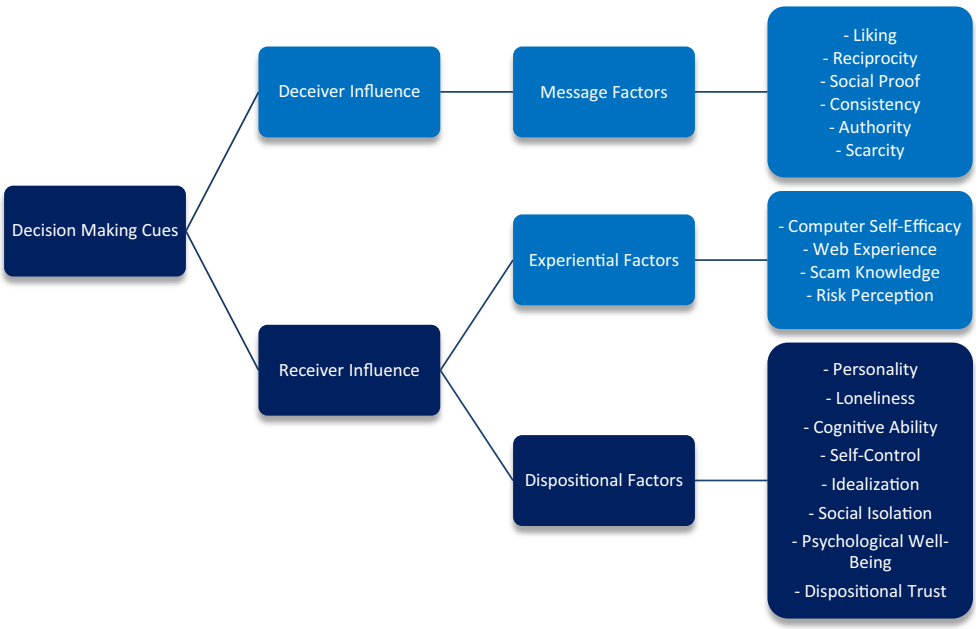

Fig. 2 Summary diagram of the variables and processes which influence an individual's ability to correctly identify fraudulent communications

Table 1 Summary table of articles focusing on message factors ($n = 6$)

Authors	Year	Location	Theory	Method	Sample	Key findings
Luo, Zhang, Burd, and Seazzu	2013	USA	Information processing; heuristics	Experimental	University staff and faculty ($n = 105$)	Phishing attacks benefit from high source credibility and time-limited responses.
Vishwanath	2016	USA	Cognitive, heuristics	Experimental	University students (study 1: $n = 64$; study 2: $n = 40$)	Mobile devices lead to more phishing attack response through screen size, cognitive demands, and habituation.
Fisher, Lea, and Evans	2013	UK	Heuristics, social influence, individual differences	Cross-sectional survey	Community research panel ($n = 103$) and community ($n = 85$)	Size of reward can (negatively) impact on decision-making; cues of trust and authority predicted scam compliance.
Harrison, Vishwanath, Ng and Rao	2015	USA	Heuristics - dual process models	Experimental	University Students (n = 85)	Richness in phishing email were heuristically processed and led to increased victimisation
Holtfreter, Reisig and Pratt	2008	USA	Self-control and rational choice	Cross-sectional survey	Community telephone sample ($n = 922$)	Low self-control leads to higher fraud victimisation; higher online consumer behaviour predicts victimisation.
Wang, Herath et al.	2012	USA	Cognitive (ELM); attention	Experimental	University students ($n = 321$)	Time limitation increase responding; deception indicators (e.g. grammar) increase attention and limit responding

knowledge and experience of computers and knowledge of fraudulent activity. Dispositional factors include personality, heuristics, and cognitive ability.

Message Factors

The 6 papers classified into this category primarily focused on how the fraudulent message was framed in order to maximise the potential for enticing a victim (Table 1). In these articles, only limited mapping onto demographic or individual factors was made. Experimental designs included 'fake' phishing emails sent out to university staff and students purporting to be from 'Information Services' requesting account verification (Luo et al. 2013). Follow-up studies of respondent demographics and personality features in these 'real-world' experiments would potentially yield important results for understanding fraud victims' behaviour, although ethically they may present some limitations.

Fischer et al. (2013) highlight four key factors that make people more likely to respond to fraudulent communications: (1) high motivation triggers in the size of the reward; (2) trust by focusing on interaction rather than message content, often generated by using 'official' notices, logos etc.; (3) social influence, including liking and reciprocation, designed to gain compliance; and (4) the scarcity or urgency of the opportunity. Utilising several waves of quantitative and qualitative studies, Fischer et al. found mixed support for these four elements associated with the message factors and indeed concluded that a fifth factor—personality—may indeed be more indicative of those people likely to predict victimisation. Fischer et al. suggest that this could be in some way linked to 'self-confidence' and an increased belief in one's ability to detect scams. Scam compliance was linked to decision-making errors—exploitation of heuristics (judgement inaccuracies)—and hence limits the exploration of message factors alone as a viable explanation of fraud. It appears that individual differences are more relevant to understanding the way messages are constructed and what processes they are likely to exploit. For example, in what way does a 'time-limited' message interact with certain individual's decision-making processes that make them more likely to respond.

The review highlighted that the content of the message was important to 'hook' the target to engaging with the deception. For example, Luo et al. (2013) demonstrated that messages with high source credibility and quality arguments are particularly effective in 'spear phishing'[1] attacks. Wang et al. (2012) also found that 'time-limited' messages (those which required a quick response) were more likely to be responded to than those which appeared less urgent; it suggests that these

[1] 'Spear phishing' differs from 'phishing' in that it is targeted at particular individuals and/or groups; the message is highly relevant and mirrors official communication styles and presentation.

'visceral triggers' reduce the cognitive effort expended upon assessing the authenticity of the message. Vishwanath (2016) extends this perspective to the use of smartphones as a means of reducing cognitive involvement in email filtering, alongside usage variables such as habituation. Responding to fraudulent messages on smartphones was found to be more probable, potentially due to increased cognitive demands and further impacted by the presentation on smaller screens and routine engagement with continued email demands whilst on the move. Certainly, fraudulent responding on smartphones is one potential additional variable to be included in future research.

Experiential Factors

A total of 7 papers were classified into the experiential category, focusing primarily on the experience and expertise of the end-user (Table 2). Knowledge of internet scams was one way in which people showed some resilience to victimisation; for example, Wright and Marett (2010) indicated that people with higher levels of computer self-efficacy, web experience, and security knowledge were less susceptible to phishing attempts. However, Internet use itself was not a protective factor; for some, usage patterns predicted whether they were likely to respond to fraudulent requests, with those people dealing with significantly high email traffic more likely to respond to messages (van Wilsem 2011; see also Vishwanath 2015). Self-control was identified as a key predictor in whether people were able to withhold responses to fraudulent requests in van Wilsem's study; what did emerge was a promising underlying pathway that linked low self-control to engaging in more online consumer behaviour generally. Interestingly, Vishwanath (2015) proposes that email behaviour—particularly habitual use—is linked to low social and emotional control and predictive of increased likelihood to respond to phishing emails.

Harrison et al. (2016a) demonstrate that individual processing styles were also indicative of the likelihood of fraud responding, although this link was moderated significantly by individual factors linked to email knowledge and experience. Similarly, Zielinska et al. (2015) compared experts and novices in their ability to conceptually link phishing characteristics, discovering the latter used much simpler mental processes in evaluating how a message might be a phishing attempt. Using a novel neurological pathway design, Zielinska and colleagues demonstrate how semantic connections become more sophisticated following experience with how phishing attacks are executed and how to take steps to avoid fraudulent victimisation. The implications for interventions are evident; in addition, the prospects to map these novice reactions to phishing attempts enable a deeper understanding of the way in which people become victims, i.e. the personal factors that limit the way in which people optimise their decision-making strategies.

Hence, a person's own competency with Internet safety cannot alone explain how they become victims of web-based fraud. Rather, it is an interaction between their ability and usage of the web and general dispositional factors, such as more deliberate and controlled information processing, which are possibly more fruitful avenues of future research in this domain. Potentially, habitual email users are susceptible—feasibly through low social control—to the way in which fraudulent messages are framed, for example, through the use of time-limited rewards, particularly when using mobile

Table 2 Summary table of articles focusing on experiential factors ($n = 7$)

Authors	Year	Location	Theory	Method	Sample	Key findings
Moody and Galleta	2011	USA	Individual differences: trust, boredom proneness, risk	Experimental	College students ($n = 632$)	Internet experience (higher usage) and risk tendency (lower financial risk takers) most predictive of phishing responses
Harrison, Vishwanath, and Rao	2016	USA	Heuristics (GCS)	Experimental	University students ($n = 192$)	Individuals with high general communicative suspicion (GCS) less likely to be phishing victim
van Wilsem	2011	Netherlands	Self-control and rational choice	Cross-sectional survey	Secondary data: large-scale longitudinal survey ($n = 6201$)	Low self-control leads to higher fraud victimisation; higher internet use predicts victimisation
Vishwanath	2015	USA	Personality, heuristics	Experimental	University students ($n = 192$)	Conscientious and habitual email responders more likely to respond to phishing requests
Zielinska, Welk, Mayhorn, and Murphy-Hill	2015	USA	Heuristics—mental models	Cross-sectional survey	Students ($n = 20$) and industry experts ($n = 15$)	Novices had simpler mental models to detect phishing; experience increased protective factors
Harrison, Svetieva, and Vishwanath	2015	USA	Cognitive (ELM); experience	Experimental	University students ($n = 113$)	Knowledge did not increase resilience to victimisation; message cues had little effect on information processing
Wright and Marett	2010	USA	Interpersonal deception theory (IDT)	Experimental	University students ($n = 446$)	Experience and training led to reduced phishing susceptibility

devices. It appears, however, that whilst message content and Internet experience have some predictive ability, the key mediating factor is individual dispositional factors that demonstrate the way in which message and experiential factors are processed.

Dispositional Factors

In reviewing the literature in the previous sections, it becomes apparent that the individual is central to the fraud victimisation process. Fischer et al. (2013) posit the question as to: '[w]hy do so many people all over the world, so often, react to completely worthless scam offers?' (p. 2060). Likewise, despite the investment in firewalls and anti-virus software, the so called semantic attacks exploit inerrant weaknesses in the system—the individual—to divulge sensitive information (Harrison et al. 2016a, b; p. 265). Workman (2008) formalises this process of *social engineering* as: '[…] techniques used to manipulate people into performing actions or divulging confidential information' (p. 662). Subsequently, the key mediating factor between the message(s) and whether experience/expertise in detecting fraud is likely to be practical are individual and personality variables.

One of the most cited papers in this domain is an early examination by Langenderfer and Shimp (2001) (Table 3). Although not focused solely on Internet-based fraud, it nonetheless identifies the 'visceral influences' that make individuals vulnerable to scams, through a process that reduces the cognitive deliberation when faced with a message. Notably, Langenderfer and Shrimp utilise Petty and Cacioppo's (1986) theory of persuasion: the elaboration likelihood model (ELM). In essence, ELM suggests that individuals who are motivated to respond to the content contained in a fraudulent message are likely to focus and be persuaded by the key messages. On the other hand, those less motivated by the content are more likely to be influenced by peripheral cues. Hence, motivation is likely to be negatively correlated with scam victimisation; the higher the level of motivation, the more likely attention will be expended upon aspects of the message and cues to deception identified. However, although widely cited, Langenderfer and Shimp (2001) rely heavily on largely anecdotal evidence for their ELM-based theory of scam compliance. Additional studies examining the relevance of ELM have found mixed support for the relevance of this individual factor relating to fraud victimisation (see Whitty 2013; Chang 2008), although Vishwanath et al. (2011) do support the ELM approach in conjunction with message and experiential influences.

In the previous section, the link between computer knowledge and self-control are identified by van Wilsem (2011). Results from Dickman's (1990) Impulsivity Inventory (DII)—as a measure of self-control—support the expected link between increased levels of fraud susceptibility. Pattinson et al. (2011) examine cognitive impulsivity alongside personality and computer familiarity. Personality was less predictive of fraud susceptibility—with the exception of agreeableness—than familiarity with computers generally (see the 'Experiential Factors" section). With regard to impulsivity, however, there was only a small relationship; generally speaking, less impulsive respondents are more able to manage potentially fraudulent messages. Using willingness to take risky investments as a proxy for low self-control, Chen et al. (2017) identify the role impulsivity has in susceptibility to responding to phishing messages, particularly those promising financial gains. Chen et al. advocate the 'unpacking' of the way in which Internet scams exploit impulsive individuals through financial rewards. Reisig and Holtfreter (2013) add additional support for the notion that lower levels of self-control are correlated to fraud victimisation.

Wider 'personality' correlates with fraud susceptibility are often featured in studies, yet many of these fail to incorporate established psychological theories from personality research and/or validated instruments. From those studies that did meet the inclusion criteria, a number attempt more exploratory research into the Big 5 personality characteristics. Hong et al. (2013) record negative correlations for openness to experience and introversion being more likely to delete legitimate emails. Hence, although these respondents were less prone to being victims of phishing messages, lower levels of trust (also measured) were predictive of general suspicion and potential rejection of genuine communication as a result. In contrast, only agreeableness was identified as a risk factor in Pattinson et al.'s (2011) research. Alternative personality inventories, for example, the HEXACO Personality Inventory (Judges et al. 2017) and the DISC Personality Questionnaire (Chuchuen and Chanvarasuth 2015), provide additional evidence for general personality influence in fraud susceptibility. Whilst some small links with potential to increase victimisation and personality factors emerge from these and other studies—for example, conscientiousness (victims have lower scores)—lead Chuchuen and Chanvarasuth (2015) caution that given the wide-range of phishing and fraudulent message content, no one personality feature is likely to predict susceptibility in isolation: '[…] there is relatively little information about the relationship between personality types and phishing techniques. However, there is some interesting literature on the relationship between decision-making that could reflect upon this area' (p. 332).

The ELM/schema models suggest that central and peripheral decision strategies are key to understanding how cues to fraudulent messages are neglected (Langenderfer and Shimp 2001). Additional heuristics and potential judgement errors have also been examined: through a content analysis of phishing emails, Chang and Chong (2010) identify the representative, availability, and affect heuristics as possible sources of decision errors. Similarly, anchoring—the tendency to use

Table 3 Summary table of articles focusing on dispositional factors ($n = 21$)

Authors	Year	Location	Theory	Method	Sample	Key findings
Langenderfer and Shimp	2001	USA	Information processing, (impulsivity/personality?), elaboration likelihood model	Cross-sectional survey	Business executives ($n = 168$)	Primarily descriptive/qualitative; age, income, and social isolation key factors in scam vulnerability
Cho, Cam, and Oltramari	2016	USA	Big 5; trust and risk perception	Probability model	Theoretical model (Stochastic Petri Nets)	Agreeableness and neuroticism impact on message perception; high neuroticism diminishes decision abilities
Chuchen and Chanvarasuth	2015	Thailand	Personality (DISC model)	Cross-sectional survey	Convenience community sample ($n = 400$)	Influence and steadiness personalities more prone to phishing; all personalities equal in response to link manipulation
Judges, Gallant, Yang, and Lee	2017	Canada	Personality, cognitive ability, and trust	Cross-sectional survey	Older adults - victims and non-victims ($n = 174$)	Victims lower scores on: cognitive ability, honesty-humility, and conscientiousness
Workman	2008	Australia/US	Social identity; obedience; impulsivity	Cross-sectional survey	Service industry employees ($n = 588$)	People high in social commitment and obedience to authority likely to elicit information
Pattinson, Jerram et al.	2011	Australia	Personality, cognitive impulsivity	Experimental	University students ($n = 117$)	High extraversion and openness, and lower impulsiveness less susceptible to phishing
Canfield, Fischhoff, and Davis	2016	USA	Signal detection theory	Experimental	Online community—mTurk (study 1: $n = 152$; study 2: $n = 100$)	More confident individuals were most likely to treat phishing messages as legitimate
Chang	2008	Australia	Elaboration likelihood model	Interpretative	Case study	Advance fee fraud exploit automatic behaviour through authority, urgency, and legitimacy
Hong, Kelley et al.	2013	USA	Personality, impulsivity	Experimental	University students ($n = 53$)	Dispositional trust, extraversion, and openness were protective factors in phishing attacks
Gavett et al.	2017	USA	Age and executive functioning	Experimental	University students ($n = 91$); community ($n = 102$)	Older adults more susceptible to phishing; executive function and older adults experience of phishing protective factor
Chang and Chong	2010	Australia	Cognitive, heuristics	Qualitative	Content analysis of phishing emails ($n = 14$)	Time limitation increase responding; autonomous and heuristic thinking styles likely to increase victimisation
	2017	USA	Self-control and rational choice	Cross-sectional survey		

Table 3 (continued)

Authors	Year	Location	Theory	Method	Sample	Key findings
Chen, Beaudoin, and Hong					Public panel survey ($n = 11,534$)	Willingness to make risky investments predicted internet fraud victimisation
Vishwanath, Herath et al.	2011	USA	Cognition (ELM; IDT); load, domain knowledge	Experimental	University students ($n = 161$)	Media use and urgency lead to higher phishing susceptibility through automatic responding
Buchanan and Whitty	2013	UK	Personality (sensation seeking, romance beliefs)	Cross-sectional survey	University students ($n = 853$); victim support ($n = 397$)	High scores on idealization led to romance scam victimisation; low openness a protective factor
Whitty	2013	UK	Cognitive (ELM); authority, triggers	Qualitative (semi-structured interviews)	Victims and online support group ($n = 20$)	ELM not explanatory in romance scams; cognitive dissonance explained lack of attention to 'red flags'
Alseadoon et al.	2013	Australia	Theory of deception (MDD); personality	Mixed (experiment and interviews)	University students ($n = 324$)	Victims fell into three categories: naïve, doubtful, and risk taker
Alseadoon, Chan et al.	2012	Australia/Saudi Arabia	Theory of deception (MDD); personality	Experimental	University students ($n = 200$)	Low email use and submissive personality less likely to suspect phishing; extraversion and openness likely to respond more
Lichtenberg, Stickney, and Paulson	2013	USA	Health and cognitive functioning	Longitudinal survey	Public panel survey ($n = 4461$)	Depression and social needs related to victimisation in older adults
Iuga, Nurse, and Erola	2016	UK	Heuristics—anchoring	Experimental	Web community sample ($n = 382$)	Real initial pages on fake website led to anchoring towards later 'real' website not phishing site
Sun, Yu, Lin, and Tseng	2016	Taiwan	Self-efficacy	Cross-sectional survey	University students ($n = 411$)	No gender differences in self-efficacy and anti-phishing behaviour
James, Boyle, and Bennett	2014	USA	Cognition; well-being	Longitudinal survey	Community panel survey ($n = 639$)	Susceptibility to fraud linked to low income, cognitive ability, well-being, social-support, and literacy
Reisig and Holtfreter	2013	USA	Self-control and rational choice	Cross-sectional survey	Community telephone sample ($n = 1958$)	Low self-control leads to higher fraud victimisation; higher internet use predicts victimisation

previous information as a base line for later decision processing—compromised the ability to identify fraudulent websites (Iuga et al. 2016). Other dispositional factors, include executive functioning (Gavett et al. 2017), theory of deception (a decision-making model; Alseadoon et al. 2012; Alseadoon et al. 2013), and cognitive health and well-being (Lichtenberg et al. 2013; James et al. 2014). Despite the obvious links to fraud, judgement and decision-making would appear to be a relatively underexplored area of research that potentially can link message and received factors in a meaningful way.

Discussion

The preamble to this review highlighted the limited use of established psychological theories in explaining Internet fraud susceptibility. From the 34 papers that met our inclusion criteria, there was still a lack of coherence in the selection of appropriate psychological principles with which to explain the increased likelihood of victimisation. In addition, there was a lack of consistency in developing useful ways in which these established psychological constructs added to our understanding of fraud conducted via the Internet. In attempting to identify the methods used by criminals and how they are targeted at specific individuals, there is a need to accurately map aspects of the message to individual differences, including Internet usage and psychological factors. This task is made more complex due to many of the papers reviewed here incorporating two or more of the three identified decision-making factors (message, experiential, and/or dispositional).

Personality theories appear to tell us very little about how people are more likely to respond to fraudulent communication via the Internet. Extravert individuals might be prone to higher levels of risk taking, but there was no clear pathway linking extraversion and fraud susceptibility (Pattinson et al. 2011). Time-limited messages might appeal to those with lower levels of social control (Reisig and Holtfreter 2013). Similarly, neuroticism increases fraud susceptibility (Cho et al. 2016), whereas conscientiousness decreases this tendency (Judges et al. 2017). These observations only loosely map onto plausible individual level explanation. In reality, it seems that the targeting of fraudulent emails—whether for phishing attacks, romance scams, or bank frauds—is done largely at random, through a high volume of communications. However, the mass release of phishing scams disguises somewhat the purposely considered message that is designed to appeal to people of specific dispositions.

What is less clear is how these messages—of which receivers negotiate several times per day—are only sometimes successful, even amongst rational and computer savvy individuals. Central versus peripheral processing may provide the most useful way to understand why people fall for scams, particularly messages that emulate official and/or genuine communications. For example, Vishwanath et al. (2011) produce a convincing account of the way in which message factors are linked to individual processing through the ELM. In addition, domain-specific knowledge also regulates the ELM process, with increased scam knowledge being linked to the attention given to email cues, i.e. a high level of elaboration likelihood. Schwarz (1990) reviews the evidence on the effect of mood upon visual information processing more generally and concluded that sad moods decreased global processing, whereas those of a happier disposition focused more on local factors. Specifically, when faced with ambiguous stimuli, mood states influenced how quickly people were likely to process information, particularly when the information was relevant to them. Additionally, people in a happy mood are more likely to pay attention to positive messages (for example, fake lottery wins). Current theories (e.g. elaboration likelihood model (ELM); see Petty and Briñol 2015) associated with mood influences on information processing suggest that happy individuals structure their response to stimuli in a top-down manner, relying more on heuristics and schemas to aid in understanding (Gasper 2004). The contrasting bottom up approach of those in less happy mood states would focus on the stimulus details more closely. Hence, we can see for our understanding of Internet fraud vulnerability that mood could be one key factor that influences how we process potentially fraudulent communications, but as yet has not received significant attention from researchers.

Practical implications concern the ability to identify individuals most at risk of fraud and provide targeted consumer education measures to help prevent victimisation. We know less about the financial situation and other background variables of fraud victims that might increase their risk of victimization. For example, does financial hardship lead people to take bigger chances with regard to false promises of prizes? Similarly, are those with physical and/or mental health problems likely to engage in dialogue with fraudsters through social isolation, anxiety, and other similar issues? Perhaps people with a predisposition for extraversion and/or risk taking may be 'happier', less likely to attend to the peripheral aspects of messages (cues to deception), and therefore be at a greater chance of being fraud victims (Gasper, 2004). Additional research with a theoretically and practically informed agenda is necessary in this important and growing field. The search terms and inclusion/exclusion criteria employed in this

review clearly focused on a relatively narrow band of studies; wider reviews of what we know about the offender and how they target victims specifically can add value to this debate. It would appear that the most used 'spam/phishing' email, however, is largely indiscriminately aimed at a wide audience hoping to catch individuals not fully processing the possibility these communications are fraudulent.

Currently, issues arise in protecting specific groups of individuals, as a high proportion of any general awareness campaign maybe targeted on people unlikely to ever fall victim, for example, elderly non-Internet users (Lea et al. 2009). This research may help bridge this gap, in that if the more vulnerable groups are identified—or are encouraged to self-identify—prevention material can be specifically targeted at them. For example, the UK National Policing '4 P's' to tackle fraud and cyber-crime; specifically, elements concerning 'protection' and 'preparation' of potential fraud victims (City of London Police 2015). Similarly, the current 'Take 5' campaign developed by The Metropolitan Police with the support of the Financial Fraud Action UK (FFA UK) highlights the importance of not immediately responding to messages. Creating a time-buffer to avoid the peripheral/heuristic interpretation of potentially fraudulent requests could potentially limit the number of responses. Experimental examinations of how people can best control their responses would appear to be a fruitful avenue on the research agenda.

Methodological Limitations

Any systematic review will undoubtedly contain some bias in terms of the search parameters employed; hence, there may be papers which are not included here that others might see as an omission. A number of papers were rejected, most notably through the stipulation that there be an established psychological theory. The question as to what was deemed 'established' is somewhat equivocal; for example, research by Van Wyk and Mason (2001) was not included because the measures for 'risk taking' and 'socialisation' were not from published scales. Similarly, Button et al. (2014) acknowledged that '[…] previous research studies have identified certain psychological traits […] This was beyond the remit of this research' (p. 400). Notably the research by Modic and colleagues is absent from the reviewed articles due to the search parameters employed here; the development of the StP-II did not fully match our criteria. Empirical examinations on the predictive validity of the StP-II are forthcoming (see Modic et al. 2018, p. 16) and if successful will provide a way of understanding and mapping personality characteristics onto fraudulent activity.

There are also some methodological considerations to be accounted for in regard to the studies themselves and in particular their ecological validity in respects to accounting for behaviour in the real world. Role play scenarios, in which participants are asked to access the account of a character and decide how they would deal with a number of emails, may suffer from expectancy/observer effects. Jones et al. (2015) argue:

> […] that the way in which these types of tasks are constructed may still prompt socially desirable responses. For example, when given the option 'type the URL into a browser window', may subsequently alert participants that this is the most sensible option compared to other options such as 'click on the link'. Parsons et al. (2014) demonstrated—using a role-play task as a measure of susceptibility—that knowledge of the nature of the study affected behaviour. Participants identified phishing emails more successfully when they had been alerted to look out for them. Such subject expectancy effects might affect the integrity of a study even more than any socially desirable bias (p. 20).

An example of a study using a role-play scenario included in the systematic review is by Pattinson et al. (2011). Jones et al. (2015) argue 'possibly, the assessment of vulnerability with the highest face validity, but clearly the most ethically challenging, would be to stimulate a genuine phishing attack by sending a fake phishing email to participants and recording whether or not they respond' (p. 22). Two examples of studies that use this method in the systematic review are by Luo et al. (2013) and Vishwanath (2016). Hence, although many studies suffer from a potential lack of ecological validity and generalizability, there is a growing corpus of studies which at the very least recognise the limitations inherent in this research domain.

Conclusion

The purpose of this systematic review was to examine the range of psychological factors associated with Internet-based fraud victimisation to identify the way in which Internet scams exploit inherently compromised human decision-making. The majority of the studies reviewed focused on 'phishing' and examined a range of factors from personality through to heuristics. Additionally, this included aspects of the message itself,

although accurately mapping these two aspects together is potentially less successful. The majority of evidence and subsequent beliefs we have regarding the psychological factors associated with vulnerability to online fraud are at best anecdotal and at worst in danger of creating misleading myths (e.g. older people are 'easy' targets). Policies designed to limit the extent and impact of fraud should clearly recognise the universal nature of compliance and that no one demographic is necessarily more or less vulnerable (Button et al. 2016). Additionally, whilst we have a steady source of material in terms of fraudulent emails, we know less about which are successful and/or why. Online fraud is relatively unique in that examples of potential criminal activity are openly available. Seemingly we are unable to stop this onslaught, but we can limit their effectiveness by increasing awareness and understanding. Through gaining an insight into how they work and with whom, the potential for law enforcement to create general and targeted crime prevention initiatives is enhanced.

Seemingly, much of the existing literature on the prevalence and prevention of Internet fraud has limited scope in terms of understanding the psychological mechanisms that lead people to become victims of these scams. Without sufficient grounding in established psychological mechanisms, it is likely that attempts to limit victimisation will be potentially flawed and/or underperform. There are a limited number of experimental designs in this field; these provide a vital understanding of how fraudulent attempts made via the Internet are able to exploit innate human frailties in decision-making. General models of risk, on the other hand, largely fail to explain why people withhold responses to very specific requests and what heuristics they use to differentiate real and fraudulent messages. Largely unexplored temporal effects, such as mood and emotion (see Gasper, 2004), provide a platform for broader contextual understanding of the fraud process.

Compliance with Ethical Standards

Conflict of Interest The authors declare that they have no conflict of interest.

Ethical Approval Ethical approval was awarded by the Department of Psychology at Aberystwyth University (#6549GGN17).

Informed Consent N/A (systematic review/analysis of existing research)

Appendix Systematic Review Technical Data

1. Review title:

i. Psychology, fraud, and risk

2. Review question

i. How have psychological mechanisms been applied to help understand the individual determinants of consumer susceptibility to online fraud victimisation?

3. Search terms

i. *Offence type*: (fraud; scam; phishing; swindles; advance-fee)
ii. *Offence subtype*: (consumer; online; internet; cyber; door; telephone; email)
iii. *Focus on victim not offender*: (victim; victimisation; victimization; victimhood; victimology; vulnerability; susceptibility; risk)
iv. *Employing psychology*: (persuasion; heuristics; decision-making; elaboration; attention; bias; social-engineering; judgement; influence; personality; mental-models; psychology; cognition)

4. Search database input fields

i. TITLE(fraud OR scam OR phishing OR swindles OR "advance fee") AND ALL(consumer OR online OR internet OR cyber OR door OR telephone OR email) AND ALL(victim OR victimisation OR victimization OR victimhood OR victimology OR vulnerability OR susceptibility OR risk) AND ALL(persuasion OR heuristics OR "decision making" OR elaboration OR attention OR bias OR "social engineering" OR judgement OR influence OR personality OR mental-models OR psychology OR cognition)

5. Possible databases

i. *Social science databases:* PsychINFO; Psych Articles; Web of knowledge core collections; social science premium collection via ProQuest; EBSCOhost; Science Direct; Wiley Online library; Scopus; PubMed; International bibliography of the social sciences; Applied social science index and abstract; Periodicals archive online via ProQuest
ii. *Criminology databases:* Criminology collection via ProQuest; Sociological abstracts; Sage criminology; Criminal justice abstracts
iii. *Grey literature:* British library collections; Google scholar; British library direct; Dissertation abstracts online; COS conference paper index; open grey www.opengrey.eu/; EthOS; WorldCat

6. Search results

Search source	Number of items	Field code used
Science Direct	356	TITLE (only offence type)
Scopus	526	TITLE (only offence type)
PsycARTICLES	3	TITLE (only offence type)
PubMed	9	TITLE (only offence type)
Web of knowledge core collection	74	TITLE (only offence type) and TS (Topic all others)
Wiley Online library	235	TITLE (only offence type)
Periodicals archive online	8	TITLE (only offence type)
EBSCOhost	88	TITLE (only offence type)
British library direct	0	TITLE (only offence type)
Open grey	0	TITLE (only offence type)
EthOS	0	TITLE (only offence type)
Google scholar	101,000	TITLE (only offence type)
WorldCat	1,567,061	TITLE (only offence type)
British library collections	20	TITLE (only offence type)
Total number of articles collected	1299	

7. Exclusion criteria applied to screening results

Exclusion criteria	Number of papers excluded
EXCLUDE 1. Duplicate article	263
EXCLUDE 2. Not published in English	1
EXCLUDE 3. Not a peer-reviewed journal article or an article found within the specified grey literature (i.e. book chapters or book reviews)	57
EXCLUDE 4. Discussed a fraud type other than online consumer fraud (i.e. mail fraud, telemarketing, corporate, intellectual property, or academic fraud)	382
EXCLUDE 5. Did not focus on the individual victims of consumer fraud (e.g. focused on technology prevention methods or the offenders)	408
EXCLUDE 6. Did not discuss individual factors (including decision-making, cognition, and personality) associated with susceptibility to fraud targeting and/or victimisation	123
EXCLUDE 7. Did not refer to an established scientifically based psychological theory (e.g. the Big 5 personality model)	31
Total number of papers included	34

References

Alseadoon I, Chan T, Foo E, Gonzales Nieto J (2012) Who is more susceptible to phishing emails?: a Saudi Arabian study. ACIS 2012: Location, location, location: Proceedings of the 23rd Australasian Conference on Information Systems 2012 (pp. 1–11). ACIS

Alseadoon IM, Othman MFI, Foo E, Chan T (2013) Typology of phishing email victims based on their behavioural response. AMCIS 2013: Anything, anywhere, anytime: Proceedings of the 19th Americas Conference on Information Systems, 5, 3716–3624

Buchanan T, Whitty MT (2014) The online dating romance scam: causes and consequences of victimhood. Psychol Crime Law 20(3):261–283

Burnes D, Henderson CR, Sheppard C, Zhao R, Pillemer K, Lachs MS (2017) Prevalence of financial fraud and scams among older adults in the United States: a systematic review and meta-analysis. Am J Public Health 107(8):13–21

Button M, Cross C (2017) Technology and fraud: the 'Fraudogenic' consequences of the internet revolution. In: McGuire M, Holt T (eds) The Routledge handbook of technology, crime and justice. Routledge, London, pp 1–5

Button M, Lewis C, Tapley J (2009) Fraud typologies and the victims of fraud: literature review. National Fraud Authority, London

Button M, McNaughton Nicholls C, Kerr J, Owen R (2014) Online frauds: learning from victims why they fall for these scams. Aust N Z J Criminol 47(3):391–408

Button M, Lewis C, Tapley J (2016) Fraud typologies and victims of fraud. National Fraud Authority, London

Chang JJ (2008) An analysis of advance fee fraud on the internet. J Financ Crime 15(1):71–81

Chang JJ, Chong MD (2010) Psychological influences in e-mail fraud. J Financ Crime 17(3):337–350

Chen H, Beaudoin CE, Hong T (2017) Securing online privacy: an empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. Comput Hum Behav 70:291–302

Cho JH, Cam H, Oltramari A (2016) Effect of personality traits on trust and risk to phishing vulnerability: modeling and analysis. Presented at the Proceedings of the IEEE CogSIMA 2016 International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support, San Diego, CA, (pp. 7–13)

Chuchuen C, Chanvarasuth P (2015) Relationship between phishing techniques and user personality model of Bangkok Internet users. Kasetsart Journal Social Sciences 36(2):322–334

City of London Police, (2015). National Policing Fraud Strategy. Available at: http://democracy.cityoflondon.gov.uk/documents/s50106/Pol_24-15_Appendix_1_Draft%20Police%20Fraud%20Strategy%20v%202.2.pdf. Accessed 24 Jun 2019

Dickman SJ (1990) Functional and dysfunctional impulsivity: personality and cognitive correlates. J Pers Soc Psychol 58:95–102

Duffield GM, Grabosky PN (2001) The psychology of fraud. Trends and Issues in Crime and Criminal Justice, 199, 1–6

Federal Bureau of Investigation (2018) Internet crime report 2018. Washington: Internet Crime Complaint Center. Available at: https://www.ic3.gov/media/annualreport/2018_IC3Report.pdf (5/6/19)

Fischer P, Lea SE, Evans KM (2013) Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam compliance. J Appl Soc Psychol 43(10):2060–2072

Gasper K (2004) Do you see what I see? Affect and visual information. Cognit Emot 18:405–421

Gavett BE, Zhao R, John SE, Bussell CA, Roberts JR, Yue C (2017) Phishing suspiciousness in older and younger adults: the role of executive functioning. PLoS One 12(2):e0171620

Harrison B, Svetieva E, Vishwanath A (2016a) Individual processing of phishing emails: how attention and elaboration protect against phishing. Online Inf Rev 40(2):265–281

Harrison B, Vishwanath A, Rao R (2016b) A user-centered approach to phishing susceptibility: the role of a suspicious personality in protecting against phishing. In System Sciences (HICSS), Proceedings of the 49th Hawaii International Conference on System Sciences (pp. 5628–5634). IEEE

Holtfreter K, Reisig MD, Pratt TC (2008) Low self-control, routine activities, and fraud victimization. Criminology 46(1):189–220

Hong KW, Kelley CM, Tembe R, Murphy-Hill E, Mayhorn CB (2013) Keeping up with the Joneses: assessing phishing susceptibility in an email task. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting (Vol. 57, No. 1, pp. 1012–1016). Sage CA: Los Angeles, CA: SAGE Publications, 57, 1012, 1016

Iuga C, Nurse JR, Erola A (2016) Baiting the hook: factors impacting susceptibility to phishing attacks. Hum-Cent Comput Info 6(1):8

Jackson SL (2017) GAO reports and senate committee on aging hearings. In: Dong X (ed) Elder abuse: research, practice, and policy. Springer, New York, pp 595–613

James BD, Boyle PA, Bennett DA (2014) Correlates of susceptibility to scams in older adults without dementia. J Elder Abuse Negl 26(2):107–122

Jones H, Towse J, Race N (2015) Susceptibility to email fraud: a review of psychological perspectives, data-collection methods, and ethical considerations. International Journal of Cyber Behavior, Psychology and Learning 5(3):13–29

Judges RA, Gallant SN, Yang L, Lee K (2017) The role of cognition, personality, and trust in fraud victimization in older adults. Front Psychol 8:588

Knutson B, Westdorp A, Kaiser E, Hommer D (2000) FMRI visualization of brain activity during a monetary incentive delay task. NeuroImage 12:20–27

Langenderfer J, Shimp TA (2001) Consumer vulnerability to scams, swindles, and fraud: a new theory of visceral influences on persuasion. Psychol Mark 18(7):763–783

Lea, S.E.G. Fischer, P. and Evans, K.M. (2009). The psychology of scams: provoking and committing errors of judgement, report for the office of fair trading. Available at: www.oft.gov.uk/shared_oft/reports/consumer_protection/oft1070.pdf. Accessed 24 Jun 2019

Lichtenberg PA, Stickney L, Paulson D (2013) Is psychological vulnerability related to the experience of fraud in older adults? Clin Gerontol 36(2):132–146

Luo XR, Zhang W, Burd S, Seazzu A (2013) Investigating phishing victimization with the heuristic-systemic model: a theoretical framework and an exploration. Comput Secur 38(C):28–38

Modic D, Lea S (2013) Scam compliance and the psychology of persuasion. Soc Sci Res Netw. Online: https://doi.org/10.2139/ssrn.2364464

Modic D, Anderson R, Palomäki J (2018) We will make you like our research: the development of a susceptibility-to-persuasion scale. PLoS One 13(3):e0194119

Moher D, Liberati A, Tetzlaff J, Altman DG (2009) Preferred Reporting Items for Systematic Reviews and Meta-Analyses: the PRISMA statement. PLoS Med 6(7):e1000097

National Audit Office (2017) Online fraud. National Audit Office, London

ONS, (2017). Overview of fraud and computer misuse statistics for England and Wales. Office for National Statistics: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudandcomputermisusestatisticsforenglandandwales/2018-01-25. Accessed 24 Jun 2019

Parsons K, McCormac A, Pattinson M, Butavicius M, Jerram C (2014) A study of information security awareness in Australian government organisations. Inf Manag Comput Secur 22(4):334–345

Pattinson MR, Jerram C, Parsons K, McCormac A, Butavicius MA (2011) Managing phishing emails: a scenario-based experiment. Paper presented at the Proceedings of the Fifth International Symposium on Human Aspects of the Information Security & Assurance HAISA (pp. 74–85)

Petty R, Cacioppo J (1986) The elaboration likelihood model of persuasion. Adv Exp Soc Psychol 19:123–205

Petty RE, Briñol P (2015) Emotion and persuasion: cognitive and meta-cognitive processes impact attitudes. Cognit Emot 29(1):1–26

Purkait S, Kumar De S, Suar D (2014) An empirical investigation of the factors that influence internet user's ability to correctly identify a phishing website. Inf Manag Comput Secur 22(3):194–234

Reisig MD, Holtfreter K (2013) Shopping fraud victimization among the elderly. J Financ Crime 20(3):324–337

Ross M, Grossmann I, Schryer E (2014) Contrary to psychological and popular opinion, there is no compelling evidence that older adults are disproportionately victimized by consumer fraud. Perspect Psychol Sci 9(4):427–442

Schwarz N (1990) Feelings as information: informational and motivational functions of affective states. In: Higgins ET, Sorrentino R (eds) Handbook of motivation and cognition: foundations of social behavior, vol 2. Guilford, New York, pp 527–561

Van Wyk J, Mason KA (2001) Investigating vulnerability and reporting behavior for consumer fraud victimization. J Contemp Crim Justice 17(4):328–345

Vishwanath A (2015) Examining the distinct antecedents of e-mail habits and its influence on the outcomes of a phishing attack. J Comput-Mediat Commun 20(5):570–584

Vishwanath A (2016) Mobile device affordance: explicating how smartphones influence the outcome of phishing attacks. Comput Hum Behav 63:198–207

Vishwanath A, Herath T, Chen R, Wang J, Rao HR (2011) Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. Decis Support Syst 51(3):576–586

Vohs KD, Mead NL, Goode MR (2006) The psychological consequences of money. Science 314(5802):1154–1156

Wang J, Herath T, Chen R, Vishwanath A, Rao HR (2012) Research article phishing susceptibility: an investigation into the processing of a targeted spear phishing email. IEEE Trans Prof Commun 55(4): 345–362

Whitty MT (2013) The scammers persuasive techniques model: development of a stage model to explain the online dating romance scam. Br J Criminol 53(4):665–684

Wright RT, Marett K (2010) The influence of experiential and dispositional factors in phishing: an empirical investigation of the deceived. J Manag Inf Syst 27(1):273–303

Zielinska OA, Welk AK, Mayhorn CB, Murphy-Hill E (2015) Exploring expert and novice mental models of phishing. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting (Vol. 59, No. 1, pp. 1132–1136). Sage CA: Los Angeles, CA: SAGE Publications